Sub B1

1. A method of providing security against unauthorized access to internal resources of a network device comprising:

receiving a digital signature at a security association manager (SAM); wherein said digital signature includes an encryption code;

said SAM requesting a de-encryption code;

said SAM de-encrypting said digital signature with said de-encryption code;

said SAM authenticating said de-encrypted digital signature; and

said SAM requesting allowed operations associated with said authenticated signature.

2. A method of providing security according to Claim 1 wherein said network device comprises a Java enabled device.

3. A method of providing security according to Claim 1 wherein said encryption code comprises a private key and said de-encryption code comprises a public key certificate associated with said private key.

4. A method of providing security according to Claim 1 further comprising:

a certificate authority receiving said request for a de-encryption code and comparing information in said request to information stored in said certificate authority.

5. A method of providing security according to Claim 4 further comprising:

said certificate authority responding to said request by sending said de-encryption code to said SAM.

6. A method of providing security according to Claim 1 further comprising:

a policy server receiving said request for allowed operations associated with said authenticated signature;

said policy server comparing said authenticated signature with information stored on said policy server; and

said policy server sending a response to said SAM indicating an access level corresponding to said authenticated signature.

7. A method of providing security according to Claim 6 further comprising:

said policy server authenticating said request for allowed operations associated with said authenticated signature prior to comparing said authenticated signature with said information stored on said policy server.

8. Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

a security association manager (SAM); configured to receive a digital signature including an encryption code;

wherein said SAM is configured to send a message including a portion of said digital signature; wherein said message includes a request for an encryption decoder;

wherein said SAM is further configured to receive a response to said message;

wherein said SAM is configured to send a digitally signed message requesting allowed operations associated with said digital signature in response to receiving said reply message.

9. Apparatus for supplying security in accordance with Claim 8 further comprising:

a certificate authority configured to receive said message from said SAM, and to send said reply; wherein said certificate authority includes

10. Apparatus for providing security according to Claim 8 wherein said network device comprises a Java enabled device.

11. Apparatus for providing security according to Claim 8 wherein said encryption code comprises a private key and said encryption decoder comprises a public key certificate associated with said private key.

12. Apparatus for providing security according to Claim 8 further comprising:

a policy server configured to receive said request for allowed operations associated with said authenticated signature;

said policy server including a comparison device configured to compare said authenticated signature with information stored on said policy server; and

said policy server being configured to send a response to said SAM indicating an access level corresponding to said authenticated signature.

13.Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

means for receiving a digital signature including an encryption code;

means for accessing a de-encryption code in electrical communication with said means for receiving; and,

means for determining allowed operations associated with said digital signature.

14. Apparatus for providing security according to Claim 13 wherein said network device comprises a Java enabled device.

15. Apparatus for providing security according to Claim 13 further comprising a downloadable file associated with said digital signature.

16. Apparatus for providing security according to Claim 13 wherein said encryption code comprises a private key.

17.Apparatus for providing security according to Claim 13 wherein said de-encryption code comprises a public key certificate.

18. Apparatus for providing security according to Claim 13 further comprising means for receiving a downloadable filing including said digital signal and assigning an access level to a java thread.